HIPAA Implementation Newsletter
Issue #18 – September 21, 2001 –
Web format with links at http://lpf.com/hipaa
Privacy & Security || Strategy

The tragic events of September 11, forced all of us to walk two paths. One to re-examine what is meaningful in our lives and the other to continue, or resume, doing what we are committed to. As time passes, the review of what is meaningful expands from a personal point of view to family and society and, for many of us, the future of our organizations. This is a time to look again at strategy and what is important for our organizations and the people we serve. It is a time to look at privacy and security for the well-being of those we serve and the private information they entrust to us.

We are usually working on two or three issues of the Newsletter at a time. As we find material, we save it, update it and publish. Issue #18, this one, has been planned for privacy, security and strategy for a number of weeks. Little did we know how timely that would be.

_____Context_____

We find it convenient to talk about HIPAA in terms of a three level structure; we were tempted to say “three ring.” At the center are transactions and code sets that are defined by and specific to HIPAA. They are not easy to implement, but the objectives are clear. At the next level are privacy and security. The standardization of codes and transmission of information

increases the risks to privacy. In addition to HIPAA, there are concurrent demands for increased privacy and security that are coming from other sources. We need to look both inward to comply with HIPAA and outward to satisfy these other demands. Privacy and security are not easy to implement and objectives will always be situational and never fully defined. The third level is operations and strategy which are impacted by HIPAA but in turn impact many of the the choices our organizations need to make as we implement HIPAA. Here again, we need to look both inward and outward. [If your email is html enabled, you will see a graphic. It may not print. If you do not see it or if it does not print, a copy is attached.]

_____Security: Qualified People_____

The events of September 11, have raised the need for security in the minds of everyone. There will be increased demands for security to be provided by a limited supply of knowledgeable and experienced people. Healthcare will find itself competing with well-financed, for-profit organizations to get the scare resources it needs. Training may offer a more realistic solution than hiring.

_____Security: Risk Assessments_____

“One of the most critical compliance success factors is the proposed HIPAA security rule’s required risk assessment. Even if the security rule is never published, covered entities must adopt rigorous security standards to ensure many of the HIPAA privacy requirements.

“The proposed security rule states that risk assessment is ‘a process whereby cost-effective security/control measures may be selected by balancing the costs of various security/control measures against the losses that would be expected if these measures were not in place.’ The security solutions should vary by entity depending on size and current level of security sophistication.

“… the best approach is to adopt a formal risk assessment model.” This was taken from an article, posted on HealthLeaders.com and provides a good outline for the conduct of a security risk assessment. If you haven’t started, this would be a good place to start. If you have started, this would be a good checklist to assure you are addressing all the critical elements. [You may have to rejoin this rather long URL to access the article.]

http://www.healthleaders.com/news/feature1.php?contentid=26663&CE_Session=ede16c2014fb57b653a900ef04bb95d0

_____Privacy: Liability_____

"The key to privacy protection is enforcement says Andrew Shen, an analyst at the Electronic Privacy Information Center, a privacy and free-speech advocacy firm in Washington. … But the bar on enforcement, and hence liability, may soon rise. There are more than 50 bills in Congress that deal with privacy (www.epic.org/privacy/bill_track.html). Some pieces of legislation, like the HIPAA, include fines for failure to comply and even harsher fines for certain offenses, like profiting from harvested medical information. …

“This combination of public outrage and increased regulation will lead to a rise in civil liability, contends Larry Ponemon, CEO of PrivacyRight Inc. in San Mateo, CA. …

"In the history of regulation, there have never been such wide-scale audits. Regulators know [financial privacy] is a massive problem. And once a regulator says there's a defect in your compliance practice, that opens a Pandora's box for class-action litigators who can take you to task on tort laws." Once again, we do not offer legal advice. We do report on legal matters from sources we consider reliable, in this case, Computer World.

http://www.computerworld.com/cwi/story/0,1199,NAV47_STO63289,00.html

_____Chief Privacy Officer_____

Healthcare organizations need a privacy officer to enforce tough new federal security regulations... "They are needed to try to help organizations prevent loss of information," said Roy Snell, CEO of the Health Care Compliance Association in an address to a security forum at NetWorld+Interop. He said a survey of 665 health care professionals found that compliance officers earn about $98,000 per year. About 80 percent of the organizations they represent have compliance programs and the budgets range from $130,000 to $690,000

“Each organization should have security policies in place and a plan for reacting to security intrusions,” Snell says. “And the policy needs to be updated and reviewed periodically -- so if an organization violates the regulations, it can demonstrate that it had taken steps to prevent it.” This apparently can be a double-edged sword because Snell also recommended checking with lawyers before documenting your precautions. "Consult legal counsel before measuring the effectiveness of your policy. It can be used against you," he warns.

Source: "Expert: Healthcare Groups Need Privacy Officers," Tim Greene, IDG, 9/14/01. as reported in PXNEWSFLASH from the Center for Social & Legal Research and Privacy & American Business, September 19, 2001

_____Fax: Security_____

The following material is taken from several emails regarding security. We offer a “common sense” endorsement but no legal advice:

“Regarding fax machines, I've heard some people state that health care organizations will have to ‘blow them up.’ I disagree, although where they are located should be well thought out, and a verification of receipt of transmission process should be implemented. Start by verifying that all preprogrammed fax numbers are indeed those of the intended recipients.

As with all aspects of HIPAA compliance you need to have documented the efforts you take to make sure that FAXes go where they are supposed to go; that there is a coversheet that states the confidential nature of the information and tells the unintended receiver what to do about receiving the information. You need to make sure that the fax machines that print the information are where the printout isn't visible to the passing public. Also, people who handle faxes need to understand that they may contain information that must be protected. You need:

1. A policy that says how you will treat faxes (confidentially).
2. Procedures for attaining confidentiality.
3. A documented process for implementing the procedures and policies (training, monitoring, auditing.)

“If this sounds simplistic, even condescending, it is because HIPAA doesn't tell you about faxes; it just says you have to protect the information and you have to figure out how to do that. It’s even conceivable you have to stop faxing to certain destinations if they can't assure you of their ability to maintain confidentiality.

_/ _/ _/ _/ _/ _/ _/ _/ _/ _/ _/ _/ _/ _/ _/ _/ _/ _/ _/

In our three level model of HIPAA, strategy is in the outer ring. The following articles will help you look over the lip of the foxhole to see what else is coming. The impact on HIPAA is indirect, but clear. HIPAA solutions must be flexible to respond to new and changing demands coming from forces beyond HIPAA’s legislation and regulations.

_____Not Just HIPAA: Disruptive Innovations_____

In 1997, Clayton Christensen published “The Innovator's Dilemma: When New Technologies Cause Great Firms to Fail.” He now has a Web site that poses the question: “While spending on health care has increased steadily over the last 40 years, spending on hospital care has been on a long-term downtrend. It seems

that hospitals aren't the pillar of the health care system that they once were. What's going on?"

September 4 -6 this year, his organization convened a consortium on health care that, among other issues, set out to begin a process that will lead to the creation of products and services that provide higher quality and greater convenience at lower cost.

http://diwire.innosight.com/
http://www.innosight.com/consortium/healthcare.html
Harvard Business Review article: "Will Disruptive Innovations Cure Health Care?"
http://www.hbsp.harvard.edu/hbsp/prod_detail.asp?R00501

_____It's Not Just HIPAA: Internet II_____

"Moore's Law is clicking over yet one more time, presenting the world with a new generation of even more powerful microprocessors and controllers ... This round is likely to be especially popular, featuring the new gigahertz chips (with their growing capacity for high-level graphics and artificial intelligence) being joined by first-generation Internet-enabled, media processor, and graphics-oriented chips ... They will be joined by new categories of hybrid devices that move complex systems--digital cameras, *__medical diagnostic equipment,__* high-speed modems--onto the surface of silicon, and thus onto the bullet train of the new boom.

"Many of these devices will enjoy their first design adoptions in the next two years. They will, in turn, power a burst of new wireless Internet devices, servers, and communications tools--just in time for the appearance, thanks to Moore's Law, of the next, even more powerful generation of chips. … Encryption, [*read security - our other topic in this issue*] that favorite activity of out-of-work Russian programmers and ex-spooks, is reaching the mainstream with the dream (and nightmare to governments everywhere) of almost perfectly private peer-to-peer transactions. …

"… Already available, if you can afford the million bucks it costs to sit at the table, is a 2.5 gigabits-per-second, double-fiber backbone, a monster architecture that is sending giant software applications, image files, and video back and forth among more than 180 universities, ***hospitals**,* and corporations. This new Internet iteration is privately funded, in large part by equipment donations from tech corporations that are using it as a test bed for future products.

http://www.forbes.com/asap/2001/0910/044.html

_____It's Not Just HIPAA: Reengineering II_____

In 1993 Michael Hammer and James Champy sold us "Reengineering the Corporation." He's back! In October Hammer will publish "The Agenda: What Every Business Must do to Dominate the Decade." "The real new economy is the customer economy. … Companies that reengineer to face the customer, to serve the customer, and to make life easier for the customer will flourish. Those that don't will perish. … Most conventional business measures are worthless. (And the others are dangerous.)" Despite the baggage reengineering has to carry, you will be hearing more about this. Forewarned is forearmed.

http://www.fastcompany.com/online/50/hammer.html

_____It's Not Just HIPAA: Leapfrog_____

The Leapfrog Group is a consortium of Fortune 500 companies and other private and public health care purchasers that provide health benefits to more than 26 million Americans and spend more than $45 billion on health care annually. The Leapfrog Group's goal is to initiate breakthroughs in the safety and quality of health care in the US. The Leapfrog Group has just launched a web-survey to gather information from hospitals nationwide about their practices on three hospital patient safety standards. "Hospitals nationwide are invited to complete

the Web survey and share their performance with their communities." When customers who spend $45 billion a year speak, their suppliers should listen.

http://www.leapfroggroup.org/hospital.htm

_____Updates_____

On the Privacy & Security page we have added: CertifiedMail, a very secure form of email, a section on "wireless security" with an article titled: Wireless Networks: Open Doors for Bad Guys and an article on the history of cookies and the impact on security
http://lpf.com/hipaa/privacy-security.html
We have added a section on "compliance" to the Background page with a comprehensive set of links to compliance resources.
http://lpf.com/hipaa/background.html#compliance-background
We have added HealthLeaders.com to the list of newsletters on the News Page
http://lpf.com/hipaa/news.html#newsletters-news

_____

To be removed from this mail list, click: mailto:hipaa@lpf.com?subject=remove

To subscribe, click: mailto:hipaa@lpf.com?subject=subscribe We appreciate it if you include information about your firm and your interests.

 Issues are posted on the Web at http://lpf.com/hipaa concurrent with email distribution. Past issues are also available there. Edited by Hal Amens hal@lpf.com

Information in the HIPAA Implementation newsletter is based on our experience as management consultants and sources we consider reliable. There are no

further warranties about accuracy or applicability. It contains neither legal nor financial advice. For that, consult appropriate professionals.

Lyon, Popanz & Forester http://lpf.com is a management consulting firm that designs and manages projects that solve management problems. Planning, program management offices and project management for HIPAA are areas of special interest.